Express Mail Label No EV 318 175 235 US

Date of Mailing November 13, 2003

PATENT
Case No. GP-303855
(2760/120)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
APPLICATION FOR UNITED STATES LETTERS PATENT

INVENTOR(S): WILLIAM L. BALL

TITLE: SYSTEM AND METHOD FOR MAINTAINING AND PROVIDING PERSONAL INFORMATION IN REAL TIME

ATTORNEYS: ANTHONY LUKE SIMON, ESQ.
GENERAL MOTORS CORPORATION
LEGAL STAFF
MAIL CODE: 482-C23-B21
300 RENAISSANCE CENTER
P.O. BOX 300
DETROIT, MICHIGAN 48265-300
(313) 665-4714

SYSTEM AND METHOD FOR MAINTAINING AND PROVIDING PERSONAL INFORMATION IN REAL TIME

FIELD OF THE INVENTION

This invention relates generally to data transmissions over a wireless communication system. More specifically, the invention relates to a key system that includes a personalized key device for storing and transmitting personal information.

BACKGROUND OF THE INVENTION

Wireless communication services for mobile vehicles, such as navigation and roadside assistance, have increased rapidly in recent years and are expanding into new service areas. One such new area of service involves summoning emergency response teams to the site of a service subscriber's vehicle after the vehicle has been involved in an accident. The request for emergency assistance may be sent via a vehicle occupant or, under some circumstances, may be sent by the vehicle.

Emergency situations that involve medical assistance often require personal medical information about the person that is being treated. However, medical history information is not always available at the site of a traffic accident for the person requiring treatment. This may be due to, for example, the patient being unable to communicate.

One current system of alerting emergency medical professionals that a patient has special medical needs requires that the patient wear a bracelet or necklace bearing an emblem, for example, a MedicAlert® bracelet. The bracelet or necklace may include an engraved telephone number and medical information. For example, the bracelet may include information indicating that the patient is diabetic, allergic to certain medications or has surgical implants,

such as a stent or a pacemaker. The telephone number that may be included on the bracelet can be used to contact a third party having additional information regarding the patient.

Though medical alert bracelets may provide needed information and peace of mind for the wearer, they do have serious limitations. One such limitation is the size of the engraving surface of the jewelry. In order to remain both wearable and fashionable, the size of the jewelry is kept small. Consequently, the size of the bracelet or necklace does not always allow a complete medical history to be engraved on the surface, resulting in the deletion of important medical information. Also, the engraved medical jewelry may not contain up to date information because updating the medical information would require the purchase of a new piece of jewelry. Another limitation of the medical alert jewelry is that they require the person to remember to wear the piece whenever they leave the home.

Other medical alert systems are inefficient in providing the medical information to emergency medical providers. One such system requires that the person carry a card containing personal information and a number to call to retrieve the medical information. This system is inefficient by requiring the medical response team to locate the card, contact the information provider using the telephone number on the card and wait for the information to be relayed to the medical provider. All of these actions waste valuable time when providing emergency medical care.

It is an object of this invention, therefore, to provide a system and method of communicating personal information to healthcare providers that overcomes the deficiencies and obstacles described above.

SUMMARY OF THE INVENTION

One aspect of the invention provides a system for providing medical information of a vehicle user to a medical provider using a wireless network. The system comprises a key device including stored medical information of a vehicle user, a telematics unit in communication with a vehicle data network, and a transient memory storage located within the vehicle and in communication with the key device and the vehicle data network. The system further includes a call center in wireless communication with the telematics unit via a wireless network. The stored medical information is transmitted from the transient storage of the vehicle via the vehicle data network to the telematics unit. Further, the medical information is transferable from the telematics unit to the call center via the wireless network.

Another aspect of the invention provides a method for providing medical information of a vehicle user to medical providers. The method comprises receiving vehicle user medical information in a key device, transmitting the medical information from the key device to a storage unit within a vehicle and transmitting the stored medical information from a telematics unit to a call center responsive to an emergency event.

Another aspect of the invention provides a system for providing medical information of a vehicle user to medical care providers. The system includes key device means for receiving and storing vehicle user medical information, vehicle storage means for receiving and storing medical information transmitted from the key device means and means for wirelessly transmitting the medical information from the vehicle storage means to a call center in response to an emergency event.

The aforementioned, and other features and advantages of the invention will become further apparent from the following detailed description of the presently preferred embodiments, read in conjunction with the accompanying drawings. The detailed description and drawings are merely illustrative of the invention rather than limiting, the scope of the invention being defined by the appended claims and equivalents thereof.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG.1 shows an illustration of one embodiment of a system for maintaining and communicating personal information through a mobile vehicle using a wireless key device, in accordance with the present invention;

FIG. 2 illustrates one embodiment of a wireless key device for a mobile vehicle, in accordance with the current invention;

FIG. 3 is a flow diagram of one embodiment of a method for maintaining and communicating personal information through a mobile vehicle using a wireless key device, in accordance with the current invention; and

FIG. 4 is a flow diagram of another embodiment of a method for maintaining and communicating personal information through a mobile vehicle using a wireless key device, in accordance with the current invention.

DETAILED DESCRIPTION OF THE PRESENTLY PREFERRED EMBODIMENTS

FIG.1 shows an illustration of one embodiment of a system for maintaining and communicating personal information through a mobile vehicle using a wireless key device, in accordance with the present invention at **100**. The wireless key system, also known as a personalized key system, is able to communicate with and transfer information to a database located within the vehicle while the keying device is in the ignition or is docked in the vehicle. Wireless key system **100** includes a mobile vehicle **110**, a key device **120**, a communications controller or telematics unit **130**, one or more wireless carrier

systems **150**, one or more communication networks **160**, one or more land networks **170**, and one or more call centers **180**. Mobile vehicle **110** is equipped with suitable hardware and software for transmitting and receiving voice and data communications.

Mobile vehicle **110** also includes ignition system **114**, in-vehicle transient storage **118** and vehicle network **146**. Ignition system **114** includes software monitor **116**. Software monitor **116** retrieves the personal data stored in key device **120** and places the data in transient storage **118** of vehicle **110**. Software monitor **116** also communicates the data placed in transient storage **118** to the telematics unit **130** via vehicle network **146**. Software monitor **116** includes suitable hardware and software for transmitting and receiving data. In one embodiment, telematics unit **130** includes transient storage **118**.

Mobile vehicle **110** also includes various types of sensors for detection of emergency events. In one embodiment, for example, the vehicle contains a sensor for detecting the deployment of the airbags. The vehicle may also include sensors that detect vehicle rollover that may occur during a traffic accident. Other sensors may detect damage to the vehicle body that may occur during an accident. These sensors may send analog or digital signals to the telematics unit **130** via vehicle network **146** upon the occurrence of the emergency event, such as, for example, the deployment of an air bag.

Key device **120** includes persistent storage memory **122** for storing personal data and a controller **124** for transmitting stored data to transient storage **118**. In one embodiment, persistent storage memory **122** is located on a key fob that is in wireless communication with ignition system **114.** In another embodiment, persistent storage memory **122** is located on a chip contained in the ignition key. In one embodiment, the personal data stored in persistent memory **122** comprises the medical history of the user. In another embodiment the personal data stored in persistent memory comprises an encrypted code.

This encrypted code would be transmitted to medical care providers and used to gain access to medical records stored on a remotely located database **192**, **194**, **196**.

Telematics unit **130** includes a digital signal processor (DSP) **132** connected to a wireless modem **134**, a global positioning system (GPS) unit **136**, an in-vehicle memory **138**, a microphone **140**, one or more speakers **142**, and an embedded or in-vehicle mobile phone **144**. DSP **132** may also be referred to as a microcontroller, controller, host processor, or vehicle communications processor. GPS unit **136** provides longitude and latitude coordinates of the vehicle. In-vehicle mobile phone **144** may be an analog, digital, dual-mode, dual-band, multi-mode or multi-band cellular phone.

DSP **132** executes various computer programs that control programming and operational modes of electronic and mechanical systems within mobile vehicle **110**. DSP **132** controls communications between telematics unit **130**, wireless carrier **150**, and call center **180**. A voice-recognition application may be installed in mobile vehicle **110** to translate human voice input through microphone **140** into digital signals. The voice-recognition application may be located in DSP **132** or other on-board electronic equipment such as a radio or electronic controller. DSP **132** may also generate and accept digital signals transmitted between key device **120** and telematics unit **130**.

Mobile vehicle **110** via a vehicle communication network **146** sends signals to various pieces of equipment and systems within mobile vehicle **110** to perform various functions such as unlocking a door, opening the trunk, setting personal comfort settings, and calling from telematics unit **130**.

Mobile vehicle **110** via telematics unit **130** sends and receives radio transmissions from wireless carrier system **150**. Wireless carrier system **150** comprises any suitable system for transmitting a signal from mobile vehicle **110** to communication network **160**.

Communication network **160** comprises services from one or more mobile telephone switching offices and wireless networks. Communication network **160** connects wireless carrier system **150** to land network **170**. Communication network **160** comprises any suitable system or collection of systems for connecting wireless carrier system **150** to mobile vehicle **110** and land network **170**.

Land network **170** may be a public-switched telephone network (PSTN) or, in another embodiment, an Internet protocol (IP) network. Land network **170** may be comprised of a wired network, an optical network, a fiber network, another wireless network, or any combination thereof. Land network **170** is connected to one or more landline telephones. Land network **170** connects communication network **160** to call center **180**. Communication network **160** and land network **170** connects wireless carrier system **150** to a communication node or call center **180**.

Call center **180** contains one or more voice and data switches **182**, one or more communication services managers **184**, one or more communication services databases **186**, one or more communication services advisors **188**, and one or more network systems **190**.

Call center **180** provides a plurality of functions. Call center **180** comprises a location where many calls are received and serviced at the same time, or where many calls are sent at the same time. The call center **180** further comprises a telematics call center, facilitating communications to and from telematics unit **130** in mobile vehicle **110**. The call center may be a voice call center, providing verbal communications between a live advisor in the call center and a subscriber in a mobile vehicle, a virtual call center having virtual advisors or a combination of both. The call center may contain each of these functions, and specifically, the call center **180** may operate using a combination of real and virtual advisors.

Call center **180** contains one or more voice and data switches **182**. Switch **182** connects land network **170** to call center **180**. Switch **182** transmits voice or data transmissions from call center **180**. Switch **182** also receives voice or data transmissions from telematics unit **130** in mobile vehicle **110** through wireless carrier system **150**, communication network **160**, and land network **170**. Switch **182** receives from or sends to one or more communication services managers **184** data transmissions via one or more networks **190**. Communication services manager **184** includes suitable hardware and software capable of providing requested communication services to telematics unit **130** in mobile vehicle **110**. Communication services manager **184** sends data transmissions to or receives data transmissions from one or more communication services databases **186** and one or more communication services advisors **188** via network system **190**. Communication services database **186** sends data transmissions to or receives data transmissions from communication services advisor **188** via network system **190**. Communication services advisor **188** receives voice or data transmissions from or sends voice or data transmissions to switch **182**. Communication services manager **184** sends data transmissions to or receives data transmissions from one or more third party databases **192, 194, 196.**

Communication services manager **184** provides one or more of a variety of services, including enrollment services, navigation assistance, directory assistance, roadside assistance, business or residential assistance, information services assistance, emergency assistance, and communications assistance. Communication services manager **184** transmits data to telematics unit **130** in mobile vehicle **110** through wireless carrier system **150**, communication network **160**, land network **170**, voice and data switch **182**, and network **190**. Communication services manager **184** may store or retrieve data and information from communication services database **186**. Communication services manager **184** provides requested information to communication services advisor **188**.

Communication services advisor **188** may be a real advisor or a virtual advisor. A real advisor is a human being in verbal communication with a user or subscriber in mobile vehicle **110** via telematics unit **130**. A virtual advisor is a synthesized voice interface responding to requests from telematics unit **130** in mobile vehicle **110**.

Communication services advisor **188** provides services to telematics unit **130** in mobile vehicle **110**. Services provided by communication services advisor **188** may include enrollment services, navigation assistance, real-time traffic advisories, directory assistance, roadside assistance, business or residential assistance, information services assistance, emergency assistance, and communications assistance. Communication services advisor **188** may communicate with telematics unit **130** in mobile vehicle **110** through wireless carrier system **150**, communication network **160**, and land network **170** using voice transmissions, or through communication services manager **184** and switch **182** using data transmissions. Switch **182** may select between voice transmissions and data transmissions.

In communicating with telematics unit **130**, key fob **120** may use wireless networking protocols such as IEEE 802.11b and IEEE 802.15 that operate in the 2.4-GHz industrial, scientific and medical (ISM) band. IEEE 802.11b, often referred to as wireless fidelity (Wi-Fi), is a standard commonly used for communication on wireless local area networks (WLAN). Key fob **120** may also use the lower-powered technology of Bluetooth™ or the IEEE 802.15 protocol, a short-range radio standard often employed in wireless personal area networks (WPAN). Bluetooth™ is particularly suited for wireless connections within 10 meters. WiFi and Bluetooth™ technology allow communication between devices located within approximately 10 to 100 meters of one another.

FIG. 2 is an illustration of one embodiment of a wireless key device for a mobile vehicle, in accordance with the present invention at **200**. In this embodiment, key device **200** is a key fob **220**. Key fob **220** is a small hardware device with a size and dimensions for comfortably fitting into a purse, on a belt, or in a pocket. The key fob may control basic services such as unlocking doors, as well as facilitate higher end services such as defining programmable steering wheel buttons, seat positions and radio stations.

In one embodiment, key fob **220** includes controller **240**, persistent memory **242**, transceiver **244**, antenna **246** and battery **248**. Key fob **220** also includes an on/off switch **228**, an LED **232** such as a green LED, and LED **234** such as a red LED. Battery **248**, may be a rechargeable battery, such as a lithium ion battery, that is recharged while the key fob is docked in a recharging device. Key fob **220** includes connector **250** that provides electrical connection to the battery charging docking mechanism. Key fob **220** also includes connector **252** to provide a connection to an external data source so that personal data may be transferred from the external data source to the persistent memory **242**. Key fob **220** may also include a directional microphone **224** and a speaker **226**.

Battery **248** provides power to run LEDs **232** and **234**, controller **240**, memory **242**, and transceiver **244**. LEDs may be used as power indicators, lighted green LED **232** meaning a charged battery and red LED **234** meaning a low-charged battery. In another embodiment, battery **248** also provides power to run microphone **224** and speaker **226**. Key fob **220** may or may not be linked to one or more keys **222.** Key fob **220** may have an intelligent key containing information about the owner and user preferences, such as favorite radio stations, personal calendar and business contact information.

Transceiver **244** may send analog or digital radio signals from the key fob **220** to transient storage of vehicle **110** via antenna **246**. In one embodiment, data is transmitted to transceiver **244** of key fob **220** wirelessly via antenna **246** and stored in persistent memory **242**.

The mobile vehicle may have several key fobs **220**, one for each driver. Each key fob **220** would contain personal medical information stored in the persistent memory **242** specific to each driver. Additional stored information may include personal comfort settings such as seat position, temperature settings, mirror alignments, and radio-station preferences. In another embodiment, key fob **220** contains personal medical information for more than one driver.

Key fob **220** includes controller **240** with computer applications that are optimized to capture data transmitted to the key fob and to transmit data to transient storage of the vehicle. Other applications may control various other operations of key fob **220**.

Associated with controller **240** is a persistent memory **242** such as a solid-state flash memory chip along with volatile memory. Memory **242** stores the personal medical records and other personal data of the driver that are transmitted to transient storage of the vehicle when the ignition system is activated at start-up. In another embodiment, persistent memory **242** stores an encryption code unique to the driver instead of the driver's medical history. Memory **242** may also store user preferences or personalized settings.

Besides communicating to the transient storage of vehicle **110** through wireless transmissions, key fob **220** can make a wired hookup via connector **252** making electrical and mechanical contact with an outside data source. The key fob **220** may be connected to a computer to download the driver's medical information from a medical provider database.

Those with skill in the art will recognize that key fob may include other embodiments and features not depicted. For example, in another embodiment, the key fob includes personal medical information for at least two individuals. For this embodiment the key fob is able to distinguish between the different drivers in order to send the appropriate data if required. This embodiment includes a biometric sensor that can distinguish one driver from another. In one such embodiment, the biometric sensor is a fingerprint sensor, as are well known in the art. In this embodiment, the driver's fingerprint is stored in the persistent memory of the key fob and is correlated to the driver's personal medical information or personal encryption code. The controller would then send the identified driver's medical information or encryption code to the transient storage of the telematics unit.

In another embodiment, the biometric sensor comprises speech recognition software and hardware as is known in the art. In this embodiment, the speech of one driver is identified and correlated to speech data stored in the key fob memory. Once the speech is identified it is correlated to that specific driver's personal medical information or encryption code.

FIG. 3 is a flow diagram of one embodiment of a method for communicating personal medical information from a mobile vehicle to emergency medical providers using a wireless communications system, and is shown generally at **300**. The method utilizes the system illustrated and described above in relation to **FIGS. 1** and **2**. The key fob includes a controller and persistent memory. The key fob is also equipped with a transceiver for wireless communications using a local short range wireless network. Wireless communications are transmitted and received using any suitable analog or digital communications technologies. The wireless communications between the key fob and the in-vehicle transient storage may be executed in accordance with a wireless communication protocol such as the IEEE 802.11 standards.

One embodiment of a method for communicating personal medical information between a mobile vehicle and a medical provider begins with storing patient data belonging to service subscriber on a database (**Block 305**). This database may be located at the service subscriber's doctor's office or hospital and may be stored on a personal computer as is well known in the art. The stored data is then transferred to the subscriber's key fob (**Block 310**). In one embodiment, the patient medical data is transferred from the database to the key fob using a wired connection between the personal computer and the key fob connector **252**. In another embodiment, the patient medical data is transferred from the personal computer to the key fob using a local short range wireless network.

Once the personal medical data has been stored on the key fob the service subscriber uses the key fob in a normal manner when used with the vehicle **110** that is part of system **100** illustrated in **FIG. 1**. For example, the user may use the key fob to lock or unlock the vehicle doors or activate a vehicle alarm. If the key is used the controller within the key fob determines whether an ignition cycle has been activated (**Block 315**). If an ignition sequence has not been initiated the method ends. If it is determined that an ignition cycle has began, the controller **240** of key fob **220** transmits the subscriber medical records to the in-vehicle transient storage **118** (**Block 320**). The medical data is transmitted to the in-vehicle transient storage using the local short range wireless network. Those with skill in the art will recognize that there are other methods of transmitting data from the key fob persistent storage to the in-vehicle transient storage. For example, the transmission may result from physical or electric communication between the persistent storage and the transient storage. In another example, the transmission may result from a Hall effect sensor, as is well known to those of ordinary skill in art, or may result from other magnetic sensors.

The personal medical information transmitted to in-vehicle transient storage is temporarily stored in the transient memory. In one embodiment, the medical information is kept in transient memory as long as the vehicle is operating. In another embodiment, the medical information is kept in transient storage for a predetermined length of time after the vehicle is turned off. In one embodiment, for example, the information is kept in transient storage for ten minutes after the vehicle is turned off. In another example, the information is kept in storage for thirty minutes post engine shut off.

During the operation of the vehicle an emergency event may occur (**Block 325**). The emergency event may be a vehicle accident that may result in damage to the vehicle. The vehicular emergency event may be detected by sensors placed within the vehicle, such as, airbag deployment sensors or other sensors that detect damage to the vehicle such as those placed on front and rear bumpers or in crumple zones of the vehicle body. The sensor would send a signal to the vehicle telematics unit 130 of vehicle 110 via vehicle network 146 that an emergency event has occurred. Telematics unit 130 would then transmit an emergency call to the call center 180 and at the same time transmit the medical information to the call center (**Block 330**). In one embodiment, the transmission of the emergency call to the call center may be initiated by a voice prompt from the telematics unit requesting instructions from the vehicle driver. For example, upon receiving an emergency event signal, the telematics unit may ask "Send emergency request?" to which the driver may say "Yes" or "No". If the driver says "Yes" the emergency call is transmitted, if the driver says "No" the method terminates. In another embodiment, if no verbal response is received from the driver, the emergency call is transmitted along with the personal medical data.

The call center would then transmit the received personal medical data to the appropriate emergency response personnel, such as, for example, emergency medical technicians and paramedics. Alternatively, the information may be transmitted to a public safety answering point (PSAP) (i.e. a 911 call center) that will then send the information to the appropriate emergency response personnel.

However, in some circumstances the emergency event (**Block 325**) may not involve the vehicle but instead may only involve the driver. For example, the driver's health may be in jeopardy such as when the driver experiences a sudden onset of an illness or a heart attack. In these situations the vehicle driver may initiate the transmission of information by pressing a button operably connected to the telematics unit **130**. In one embodiment, telematics unit **130** includes an emergency button that, when depressed transmits a request for emergency assistance. In another embodiment, the emergency request may be voice activated. Once the emergency request has been initiated, the telematics unit **130** transmits the personal medical information located in transient storage **118** along with the request for emergency assistance (**Block 330**). The call center will then transmit the personal medical information to the appropriate personal as discussed above (**Block 335**).

FIG. 4 is a flow diagram of another embodiment of a method for communicating personal medical information from a mobile vehicle to emergency medical providers using a wireless communications system, and is shown generally at **400**. The method utilizes the system illustrated and described above in relation to **FIGS. 1** and **2**. The key fob includes a controller and persistent memory. The key fob is also equipped with a transceiver for wireless communications using a local short range wireless network. Wireless communications are transmitted and received using any suitable analog or digital communications technologies. The wireless communications between the key fob and the in-vehicle transient storage may be executed in accordance with a wireless communication protocol such as the IEEE 802.11 standards.

One embodiment of a method for communicating personal medical information between a mobile vehicle and a medical provider begins with storing patient data belonging to service subscriber on a database (**Block 405**). This database **192**, **194**, **196** may be located at the service subscriber's doctor's office or hospital or may be located at a third party data repository. The personal medical records stored in the database would be associated with a unique encryption code. The encryption code can be used to gain access to specific patient records.

The encryption code is then transferred to and stored on the subscriber's key fob (**Block 410**). In one embodiment, the encryption code is transferred from the database to the key fob using a wired connection between the computer housing the database and the key fob connector **252**. In another embodiment, the encryption code is transferred from the database housing the encryption code to the key fob using a local short range wireless network.

Once the encryption code has been stored on the key fob the service subscriber uses the key fob in a normal manner when used with the vehicle **110** that is part of system **100** illustrated in **FIG. 1**. For example, the user may use the key fob to lock or unlock the vehicle doors or activate a vehicle alarm. If the key is used the controller within the key fob determines whether an ignition cycle has been activated (**Block 415**). If an ignition sequence has not been initiated the method ends. If it is determined that an ignition cycle has began, the controller **240** of key fob **220** transmits the subscriber encryption code to the in-vehicle transient storage **118** (**Block 420**). The encryption code is transmitted to the in-vehicle transient storage using the local short range wireless network. Those with skill in the art will recognize that there are other methods of transmitting data from the key fob persistent storage to the in-vehicle transient storage.

The encryption code transmitted to in-vehicle transient storage is temporarily stored in the transient memory. In one embodiment, the encryption code is kept in transient memory as long as the vehicle is operating. In another embodiment, the encryption code is kept in transient storage for a predetermined length of time after the vehicle is turned off. In one embodiment, for example, the encryption code is kept in transient storage for ten minutes after the vehicle is turned off. In another example, the encryption code is kept in storage for thirty minutes post engine shut off.

During the operation of the vehicle an emergency event may occur (**Block 425**). The emergency event may be a vehicle accident that may result in damage to the vehicle. The vehicular emergency event may be detected by sensors placed within the vehicle, such as, airbag deployment sensors or other sensors that detect damage to the vehicle such as those placed on front and rear bumpers or in crumple zones of the vehicle body. The sensor would send a signal to the vehicle telematics unit **130** of vehicle **110** via vehicle network **146** that an emergency event has occurred. Telematics unit **130** would then transmit an emergency call to the call center **180** and at the same time transmit the encryption code to the call center (**Block 430**).

The call center would then transmit the encryption code to the appropriate emergency response personnel, such as, for example, emergency medical technicians and paramedics. Alternatively, the information may be transmitted to a public safety answering point (PSAP) (i.e. a 911 call center) that will then send the encryption code to the appropriate emergency response personnel.

However, in some circumstances the emergency event (**Block 425**) may not involve the vehicle but instead may only involve the driver. For example, the driver's health may be in jeopardy such as when the driver experiences a sudden onset of an illness or a heart attack. In these situations the vehicle driver may initiate the transmission of encryption code by pressing a button operably connected to the telematics unit **130**. In one embodiment, telematics unit **130** includes an emergency button that, when depressed transmits a request for emergency assistance. In another embodiment, the emergency request may be voice activated. Once the emergency request has been initiated, the telematics unit **130** transmits the encryption code located in transient storage **118** along with the request for emergency assistance (**Block 430**). The call center will then transmit the encryption code to the appropriate personal as discussed above (**Block 435**).

The emergency medical providers would then use the encryption code to access the medical information for the service subscriber. This may be done in route to the vehicle of the service subscriber or it may be done at the scene of the accident or, alternatively, the information may be accessed at the hospital once the service subscriber arrives.

In another embodiment of the system for communicating medical information from a vehicle to the medical provider the key device comprises a key with an embedded microchip. Keys having microchips are known in the art for use as a theft deterrent. In this embodiment the embedded chip has persistent memory sufficient for storing either the medical information or the encryption code. The medical information or encryption code would be transferred to transient memory upon starting the vehicle.

In still another embodiment, the key device is similar to a credit card, the card having the medical information or encryption code stored on the card. When the card is used to start the vehicle, the medical information or encryption code would be transferred to transient storage.

While the embodiments of the invention disclosed herein are presently considered to be preferred, various changes and modifications can be made without departing from the spirit and scope of the invention. The scope of the invention is indicated in the appended claims, and all changes that come within the meaning and range of equivalents are intended to be embraced therein.